UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN RE CROP PROTECTION PRODUCTS LOYALTY PROGRAM ANTITRUST LITIGATION This document relates to: ALL ACTIONS	Case No: 1:23-md-3062-TDS-JEP

STIPULATED ORDER RE: DISCOVERY OF ELECTRONICALLY STORED INFORMATION

1. Purpose

The Parties to the above-captioned case (the "Action"), through their respective counsel, agree that the terms and conditions of this Order Regarding Discovery of Electronically Stored Information ("ESI Stipulation and Order") shall govern discovery of electronically stored information ("ESI," as defined below), as a supplement to the Federal Rules of Civil Procedure, the Rules of Practice and Procedure of the United States District Court for the Middle District of North Carolina, and any other applicable orders and rules.

2. Definitions

2.1 "Document" shall have the same meaning and scope as it has in Federal Rule of Civil Procedure 34(a)(1)(A).

2.2 "ESI" is an abbreviation of "electronically stored information" and shall have the same meaning and scope as it has in Federal Rule of Civil Procedure 34(a)(1)(A).

2.3 "Non-Party" means any natural person, partnership, corporation, association, or other legal entity not named as a Party to the Action.

2.4 "Party" means any Plaintiff or Defendant in the Action. Parties means collectively the Plaintiffs and Defendants in the Action.

2.5 "Producing Party" means a Party or Non-Party that produces information, Documents, or ESI in the Action.

2.6 "Requesting Party" means a Party requesting, or otherwise entitled to receive, information, Documents, or ESI from a Party or Non-Party in the Action.

3. General Provisions

The production specifications set forth in this ESI Stipulation and Order apply to Documents and ESI that are to be produced in the first instance in the Action. To the extent any Producing Party reproduces Documents or ESI previously produced to it by any Party or Non-Party during a pre-complaint government investigation of the subject matter of the Action, that Party may reproduce such Documents or ESI in the manner in

which it was originally produced. No Party is obligated to reformat a reproduction of any prior production in accordance with the production specifications in this ESI Stipulation and Order.

4. Preservation

Each Party will continue its retention practices with regards to all Documents and ESI and will take reasonable and proportionate steps to preserve relevant and discoverable Documents and ESI in compliance with duties to preserve material under the Federal Rules of Evidence and the Federal Rules of Civil Procedure. The Parties agree to meet and confer to the extent any Party seeks limitations on the scope of its preservation duties.

5. Collection and Review

5.1 The Parties agree that in responding to an initial and any subsequent Fed. R. Civ. P. 34 request, they will meet and confer about methods to search ESI in order to identify ESI that is subject to production and discovery and filter out ESI that is not subject to discovery, including the selection of appropriate custodians, custodial and non-custodial sources, date ranges, file types, or any additional proposed method to cull documents for review (*e.g.*, search terms, technology-assisted review, predictive coding, artificial intelligence).

5.2 Search Terms. If a Producing Party intends to use search terms to limit its collection, review, or production of ESI, that Party or Non-Party shall

disclose to the Requesting Party the collections of ESI for which it proposes to use search terms and the search terms that it proposes to use for each collection of ESI. The Producing Party shall also make disclosures reasonably necessary for the Requesting Party to assess the efficacy of the proposed search terms, including, but not limited to, (1) the number of documents responsive to the search terms collectively; (2) the number of documents that hit on a specific search term and no other search terms (*i.e.*, unique hit count); and (3) the number of documents responsive to each proposed search term. After receipt of the search terms and disclosures set forth above, the Requesting Party shall raise any concerns and propose any additions or modification it may have to the search terms. The Parties and any Non-Parties shall meet and confer in good faith regarding any proposed changes, and provide updated search term disclosures, consistent with the disclosures described above, addressing proposed additional search terms. Any disputes regarding the use of search terms that cannot be so resolved may be consequently raised with the Court.

5.3 Technology Assisted Review ("TAR"). If any Party or Non-Party wishes to use TAR (including predictive coding or artificial intelligence) to determine whether Documents or ESI are responsive or to otherwise limit the Documents or ESI that it produces, it shall notify the Requesting Party and provide it a proposed TAR protocol, before implementing any TAR

protocol. That TAR protocol shall identify the TAR software name and version and the types of metrics available during the training, overview of the review and training workflow, quality control, and validation processes. These metrics shall include a proposed recall level and a proposed confidence level. The protocol should also include a proposal for non-responsive sampling analysis, with all appropriate metrics for such analysis. After receipt of the TAR protocol set forth above, the Requesting Party shall raise any concerns and propose any additions or modification it may have. The relevant Parties and any Non-Parties shall meet and confer in good faith regarding any proposed changes. Any disputes regarding the use of TAR that cannot be so resolved may be consequently raised with the Court.

Notwithstanding the above, Documents or ESI that are found only in hard copy, are data sets, or are uncategorizable (i.e., Documents that do not have sufficient text, or too much text, to be categorized using TAR) will be reviewed manually, or, in the case of junk files, may be reviewed through statistical sampling.

5.4 Each Producing Party shall use its best efforts to filter out common system files and application executable files by using a commercially reasonable hash identification process. Hash values that may be filtered out during this

process are located in the National Software Reference Library ("NSRL") NIST hash set list.

5.5 Embedded Objects. Each Producing Party may, at their reasonable discretion, filter out embedded objects.

5.6 De-Duplication. Removal of duplicate Documents should only be done on exact duplicated Documents (based on MD5 or SHA-1 hash values, at the family level). Attachments should not be eliminated as duplicates for purposes of production, unless the parent e-mail and all attachments are also duplicates. When applying de-duplication, metadata identifying all custodians in possession of each Document that is removed as a duplicate must be provided in the "Alternative Custodian" metadata field, to the extent applicable. Additionally, all BCC recipients whose names would have been included in the BCC metadata field, to the extent such metadata exists, but are excluded because of de-duplication, must be identified in the BCC metadata field specified in Appendix 1. In the event of rolling production of Documents or ESI, the Producing Party will, as needed supplement the load files with updated Alternative Custodian and file path information, as well as update BCC information to the extent such metadata

exists. Duplicate custodian information may be provided by a metadata overlay and will be provided by a Producing Party on an ongoing basis.

5.7 Email Threading. Where multiple email messages are part of a single chain or "thread," a Producing Party is only required to produce the most inclusive message ("Last In Time Email") and need not produce earlier, less inclusive email messages or "thread members" that are fully contained, including attachments and inline objects (including inline images and hyperlinks) and including identical text, identical subject(s), identical senders and recipients (including in "to," "cc," and "bcc" fields), within the Last In Time Email. Only email messages for which all inline objects, text, subject(s), senders, recipients, and attachments are fully contained in and identical to the relevant portion of the Last In Time Email will be considered less inclusive email messages that need not be produced.

5.8 Hardcopy Documents. In scanning hardcopy Documents, distinct Documents should not be merged into a single record, and single Documents should not be split into multiple records (*i.e.*, hardcopy Documents should be logically unitized).

5.9 Password Protected Files. The Producing Party shall make reasonable efforts to ensure that encrypted or password-protected Documents are processed for review and production under the requirements of this ESI Stipulation and Order, and that the decrypted Document is produced if

responsive and not privileged. To the extent such a Document is not successfully processed and is either attached to another Document meeting production criteria or itself has extractable metadata meeting production criteria, the Producing Party agrees to: (i) produce a slipsheet for each encrypted or password-protected Document that cannot be successfully processed indicating that the Document cannot be decrypted; and (ii) provide the metadata for the Document required by Exhibit 1 to the extent it can be reasonably extracted from the file in its encrypted form. The encrypted native version of the Document or ESI need not be produced.

5.10 Filtering. If a Producing Party proposes to apply filters to limit Documents and ESI that is collected for processing and review other than those described in this Order, the Producing Party shall advise all Requesting Parties and the Requesting and Producing Parties shall meet and confer regarding such additional proposed filters.

6. Production Format

Producing Parties produce Documents and ESI in the formats described in Appendix 1 to this Order. If particular Documents or ESI warrant a different format, the Parties and any Non-Parties shall cooperate to arrange for the mutually acceptable production of such Documents or ESI. To the extent practicable, Producing Parties shall not materially degrade the searchability of Documents or ESI as part of the production process.

7. **Privilege Log**

7.1 The Producing Party shall provide the Requesting Party with a log in Excel format of the Documents withheld for privilege containing the following information, to the extent reasonably available: document number, custodian, author/sender, recipient, CC recipient, BCC recipient, date sent, date created, date last modified, file path(s), last edited by, hash value, file name, subject, and time, subject, Privilege Basis and Privilege Justification.

7.2 "Privilege Basis" refers to the legal basis for withholding the document (*e.g.*, Attorney-Client Communication, Attorney Work Product). "Privilege Justification" refers to a description justifying the Privilege Basis, including as appropriate, the subject matter of the legal advice, and/or the litigation matter for which the Document was prepared. To the extent a common interest is asserted, that shall be indicated in the Privilege Basis. The same Privilege Justification may be used for multiple Documents so long as the Privilege Justification is accurate.

7.3 Parties must identify lawyers and third parties on their privilege logs. Parties must identify lawyers in one of two ways: (1) they may provide the other Party with a list with the privilege log that names the lawyers on the log, identifying whether they are in-house or external counsel, or (2) they may designate in-house attorney names with an asterisk and designate outside counsel attorney names with a double asterisk. To the extent

attorneys are not identified in the above fields, they shall be identified in a separate "Attorneys" field.

7.4 Information to be included in the log may be generated from available Metadata so long as: (a) it is reliable and does not contain information that is privileged or protected; and (b) the following additional metadata fields are included (if reasonably available): (i) file path(s); (ii) last edited by; (iii) hash value; (iv) file name; and (v) subject.

7.5 A single Document containing multiple Email messages (*i.e.*, an Email chain) may be logged as a single entry with all sender and recipient information for only the most inclusive Email messagee if the entire chain is privileged. If only part of a chain is privileged, the privileged content should be redacted and the remaining content in the chain should be produced.

7.6 A Document Family (*e.g.*, an Email and its attachments) may be logged as a single entry so long as the entire Family is privileged and the log entry accurately describes both the Parent and its attachment(s) in the manner required by Rule 26(b)(5)(A)(ii).

7.7 Documents that need not be logged are identified in the Protective Order.

7.8 Notwithstanding the foregoing, log entries contained in final privilege logs produced during the Government Plaintiffs' pre-complaint investigations

need not be included in subsequent privilege logs and need not automatically be reformatted consistent with this ESI Stipulation and Order.

IT IS THEREFORE ORDERED that the Joint Motion for Entry of a Stipulated Order Regarding the Discovery of Electronically Stored Information [Doc. #115] is GRANTED and the Stipulated Order is ADOPTED as set out above.

This, the 28th day of May, 2024.

/s/ Joi Elizabeth Peake
United States Magistrate Judge

APPENDIX 1: PRODUCTION FORMAT

1. A cover letter shall be included with each production and shall include information sufficient to identify all accompanying media (hard drive, thumb drive, DVD, CD, secure FTP), shall identify each production on such media by assigning a Production Volume name or number, shall include the Bates range for the Documents produced in each volume, and shall include a list of load file fields in the order in which they are organized in the load file.
2. Except for privileged material, the Producing Party will produce each responsive document in its entirety by including all shared-drive hyperlinks (if reasonably available) and attachments and all pages, regardless of whether they directly relate to the specified subject matter. Attachments must be produced along with the document to which they are attached and/or linked. Hyperlinked documents will be produced along with the document that links to them to the extent the hyperlinked document can be reasonably and automatically exported with the original document at the time of collection. In the event that a hyperlinked document is not produced with the file to which it is linked, the Producing Party will meet and confer about producing it in response to a specific request from the Requesting Party. Copies that differ in any respect from an original (because, by way of example only, handwritten or printed notations have been added) should be produced separately.

3. Form of Production. Documents stored in electronic or hard-copy formats in the ordinary course of business shall be submitted in the following electronic format, in color to the extent kept in color in the ordinary course, provided that such copies are true, correct, and complete copies of the original documents:

    a) Submit spreadsheet (e.g., Excel), presentation (e.g., PowerPoint), and media (e.g., .mp4), and word processing documents with tracked changes (but only if track changes information do not appear in image format productions), files in native format with extracted text and metadata, except if any such files are being redacted, in which case redacted presentation files may be produced as single page 300 DPI TIFF/ JPG images (JPG if in color). Delimited text files and files exceeding 999 pages when imaged may also be produced in native format. For each native file produced, the production will include a *.tiff image slipsheet indicating the production number of the native file and the confidentiality designation, and stating "File Provided Natively." Submit the following metadata and information for native files as applicable (to the extent reasonably available):

Metadata/Document Information	Description
Alternative Custodian	List of custodians where the document has been removed as a duplicate.
Bates Begin	Beginning Bates number of the email.
Bates End	Bates number of the last page of the email.
Beg Attach	First Bates number of attachment range.
End Attach	Ending Bates number of attachment range.
Custodian	Name of the person from whom the email was obtained.

Metadata/Document Information	Description
Email BCC	Names of person(s) blind copied on the email.
Email CC	Names of person(s) copied on the email.
Email Date Received	Date the email was received. [MM/DD/YYYY]
Email Date Sent	Date the email was sent. [MM/DD/YYYY]
Email From	Names of the person who authored the email.
Email Message ID	Microsoft Outlook Message ID or similar value in other message systems.

Metadata/Document Information	Description
Email Subject	Subject line of the Email or Calendar Invite
Email Time Received	Time email was received. [HH:MM:SS AM/PM]
Email To	Recipients(s) of the email.
Email Time Sent	Time email was sent. [HH:MM:SS AM/PM]
Page count	Number of pages in record.
File size	Size of document in KB.
File Extension	File extension type (*e.g.*, docx, xlsx).

Metadata/Document Information	Description
Record Type	Indicates form of record: E-Doc, E-Doc Attachment, Email, Email Attachment, HardCopy, Calendar Appt, Text Message, Chat Message etc.
Folder	File path/folder location of email.
Hash	Identifying value used for deduplication – typically SHA1 or MD5.
Redaction	Indicates Yes or No status regarding document redactions.
Text Link	Relative path to submitted text file. Example: \TEXT\001\FTC0003090.txt
Confidentiality	Confidentiality designation pursuant to the Protective Order.

b) Submit emails in 300 DPI TIFF (Group IV) format with extracted text and the following metadata and information as applicable (to the extent reasonably available):

Metadata/Document Information	**Description**
Alternative Custodian	List of custodians where the document has been removed as a duplicate.
Bates Begin	Beginning Bates number of the email.
Bates End	Bates number of the last page of the email.
Beg Attach	First Bates number of attachment range.
End Attach	Ending Bates number of attachment range.

Metadata/Document Information	Description
Custodian	Name of the person from whom the email was obtained.
Email BCC	Names of person(s) blind copied on the email.
Email CC	Names of person(s) copied on the email.
Email Date Received	Date the email was received. [MM/DD/YYYY]
Email Date Sent	Date the email was sent. [MM/DD/YYYY]
Email From	Names of the person who authored the email.

Metadata/Document Information	Description
Email Message ID	Microsoft Outlook Message ID or similar value in other message systems.
Email Subject	Subject line of the Email or Calendar Invite
Email Time Received	Time email was received. [HH:MM:SS AM/PM]
Email To	Recipients(s) of the email.
Email Time Sent	Time email was sent. [HH:MM:SS AM/PM]
Page count	Number of pages in record.
File size	Size of document in KB.

Metadata/Document Information	Description
File Extension	File extension type (*e.g.*, docx, xlsx).
Record Type	Indicates form of record: E-Doc, E-Doc Attachment, Email, Email Attachment, HardCopy, Calendar Appt, Text Message, Chat Message etc.
Folder	File path/folder location of email.
Hash	Identifying value used for deduplication – typically SHA1 or MD5.
Redaction	Indicates Yes or No status regarding document redactions.
Text Link	Relative path to submitted text file. Example: \TEXT\001\FTC0003090.txt
Confidentiality	Confidentiality designation pursuant to the Protective Order.

c) Submit email attachments other than those described in subpart in subpart 3.a) in 300 DPI TIFF (Group IV) format. For all email attachments, provide extracted text and the following metadata and information as applicable (if reasonably available):

Metadata/Document Information	**Description**
Alternative Custodian	List of custodians where the document has been removed as a duplicate.
Bates Begin	Beginning Bates number of the document.
Bates End	Last Bates number of the document.
Beg Attach	First Bates number of attachment range.
End Attach	Ending Bates number of attachment range.

Metadata/Document Information	Description
Custodian	Name of person from whom the file was obtained.
Date Created	Date the file was created. [MM/DD/YYY]
Date Modified	Date the file was last changed and saved. [MM/DD/YYYY]
Page count	Number of pages in record.
File size	Size of document in KB.
File Extension	File extension type (*e.g.*, docx, xlsx).
Filename with extension	Name of the original native file with file extension.

Metadata/Document Information	Description
Record Type	Indicates form of record: E-Doc, E-Doc Attachment, Email, Email Attachment, HardCopy, Calendar Appt, Text Message, Chat Message etc.
Hash	Identifying value used for deduplication – typically SHA1 or MD5.
Author	Author field value extracted from the metadata of a native file
Last Author	Last Saved By field value extracted from metadata of a native file
Redaction	Indicates Yes or No status regarding document redactions.
Native Link	Relative file path to submitted native or near native files. Example: \NATIVES\001\FTC0003090.xls

Metadata/Document Information	Description
Parent ID	Document ID or beginning Bates number of the parent email.
Text Link	Relative path to submitted text file. Example: \TEXT\001\FTC0003090.txt
Time Created	Time file was created. [HH:MM:SS AM/PM]
Time Modified	Time file was saved. [HH:MM:SS AM/PM]
Confidentiality	Confidentiality designation pursuant to Protective Order.

d) To the extent instant messages (*e.g.*, text messages, WhatsApp, Slack, iMessage, Teams, G-Chat, Bloomberg, etc.) are produced, a Party shall produce such messages such that individual messages are grouped into threads (*i.e.*, continuous conversations between one or more individuals) of

24 hours to allow for the full context of conversations to be visible. Submit instant messages in native or TIFF Relativity Short Message Format ("RSMF") accompanied by extracted text if available, or OCR, and the following metadata (if reasonably available) and meet and confer regarding any additional metadata fields that could be produced, depending on the type of message:

Metadata/Document Information	**Description**
Instant Message Type	The type of electronic message (*e.g.*, Text Message, Slack, Microsoft Teams, Instant Bloomberg, etc.)
Instant Message Participants	Senders, recipients, subscribers, or others who have the ability to participate in a group message or channel
Instant Message Subject	Subject or name of the messaging thread or topic, if any
Instant Message Channel	Name of persistent messaging group or chat room, if any
Instant Message Date	Date of last instant message in the 24-hour thread
Confidentiality	Confidentiality designation pursuant to the Protective Order.

e) Submit all other electronic documents, other than those described in subpart 3.a), in 300 DPI TIFF (Group IV) format accompanied by extracted text and the following metadata and information as applicable (if reasonably available):

Metadata/Document Information	Description
Alternative Custodian	List of custodians where the document has been removed as a duplicate.
Bates Begin	Beginning Bates number of the document.
Bates End	Last Bates number of the document.
Beg Attach	First Bates number of attachment range.
End Attach	Ending Bates number of attachment range.
Custodian	Name of the original custodian of the file.

Metadata/Document Information	Description
Date Created	Date the file was created. [MM/DD/YYY]
Date Modified	Date the file was last changed and saved. [MM/DD/YYYY HH:MM:SS AM/PM]
Record Type	Indicates form of record: E-Doc, E-Doc Attachment, Email, Email Attachment, HardCopy, Calendar Appt, Text Message, Chat Message etc.
Author	Author field value extracted from the metadata of a native file
Last Author	Last Saved By field value extracted from metadata of a native file
Redaction	Indicates Yes or No status regarding document redactions.
Page count	Number of pages in record.

Metadata/Document Information	Description
File size	Size of document in KB.
File Extension	File extension type (*e.g.*, docx, xlsx).
Filename with extension	Name of the original native file with file extension.
Hash	Identifying value used for deduplication – typically SHA1 or MD5.
Originating Path	File path of the file as it resided in its original environment.
Production Link	Relative path to submitted native or near native files. Example: \NATIVES\001\FTC0003090.xls

Metadata/Document Information	Description
Text Link	Relative path to submitted text file. Example: \TEXT\001\FTC-0003090.txt
Time Created	Time file was created. [HH:MM:SS AM/PM]
Time Modified	Time file was saved. [HH:MM:SS AM/PM]
Confidentiality	Confidentiality designation pursuant to the Protective Order.

f) Submit documents stored in hard copy in 300 DPI TIFF (Group IV) format accompanied by OCR with the following information:

Metadata/Document Information	Description
Bates Begin	Beginning Bates number of the document.
Bates End	Bates number of the last page of the document.
Record Type	Indicates form of record: E-Doc, E-Doc Attachment, Email, Email Attachment, HardCopy, Calendar Appt, Text Message, Chat Message etc.
Page count	Number of pages in record.
Redaction	Indicates Yes or No status regarding document redactions.
Custodian	Name of person from whom the file was obtained.
Confidentiality	Confidentiality designation pursuant to the Protective Order.

g) Submit redacted documents in TIFF/JPG format accompanied by extracted text or OCR with the metadata and information required by relevant document type in subparts 3.a-f) above.

h) Documents produced as TIFFs/JPGs will show any and all non-privileged text, hidden content, and images that would be visible to the reader using the native software that created the document, including any tracked changes, comments, speaker notes, and hidden content.

4. For requests in which responsive information is contained in a database (*e.g.*, Microsoft Access) or other structured or aggregated data source or otherwise maintained by an application, the Parties shall meet and confer as to whether a Party may produce relevant information by generating one or more reports used in the ordinary course of business. If the Requesting Party believes that the generation of ordinary course reports is not adequate, the relevant Parties agree to meet and confer to discuss alternative forms of production. If the relevant Parties cannot reach agreement, the matter may be submitted to the Court for resolution.

5. Compressed file types (e.g., .ZIP, .RAR, .CAB, .Z) should be decompressed so that the lowest level document or file is extracted.

6. Produce ESI submissions as follows:

a) For productions over 500 gigabytes, use an External Hard Disc Drive (stand-alone portable or hard drive enclosure) or USB Flash Drive in Microsoft Windows-compatible, uncompressed data format.

b) For productions under 500 gigabytes, submissions may be transmitted electronically via secure File Transfer Protocol, such as Kiteworks or Globalscape.

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN RE CROP PROTECTION PRODUCTS LOYALTY PROGRAM ANTITRUST LITIGATION This document relates to: ALL ACTIONS	Case No: 1:23-md-3062-TDS-JEP

STIPULATED ORDER RE: DISCOVERY OF ELECTRONICALLY STORED INFORMATION

1. Purpose

The Parties to the above-captioned case (the "Action"), through their respective counsel, agree that the terms and conditions of this Order Regarding Discovery of Electronically Stored Information ("ESI Stipulation and Order") shall govern discovery of electronically stored information ("ESI," as defined below), as a supplement to the Federal Rules of Civil Procedure, the Rules of Practice and Procedure of the United States District Court for the Middle District of North Carolina, and any other applicable orders and rules.

2. Definitions

2.1 "Document" shall have the same meaning and scope as it has in Federal Rule of Civil Procedure 34(a)(1)(A).

2.2 "ESI" is an abbreviation of "electronically stored information" and shall have the same meaning and scope as it has in Federal Rule of Civil Procedure 34(a)(1)(A).

2.3 "Non-Party" means any natural person, partnership, corporation, association, or other legal entity not named as a Party to the Action.

2.4 "Party" means any Plaintiff or Defendant in the Action. Parties means collectively the Plaintiffs and Defendants in the Action.

2.5 "Producing Party" means a Party or Non-Party that produces information, Documents, or ESI in the Action.

2.6 "Requesting Party" means a Party requesting, or otherwise entitled to receive, information, Documents, or ESI from a Party or Non-Party in the Action.

3. General Provisions

The production specifications set forth in this ESI Stipulation and Order apply to Documents and ESI that are to be produced in the first instance in the Action. To the extent any Producing Party reproduces Documents or ESI previously produced to it by any Party or Non-Party during a pre-complaint government investigation of the subject matter of the Action, that Party may reproduce such Documents or ESI in the manner in

which it was originally produced. No Party is obligated to reformat a reproduction of any prior production in accordance with the production specifications in this ESI Stipulation and Order.

4. Preservation

Each Party will continue its retention practices with regards to all Documents and ESI and will take reasonable and proportionate steps to preserve relevant and discoverable Documents and ESI in compliance with duties to preserve material under the Federal Rules of Evidence and the Federal Rules of Civil Procedure. The Parties agree to meet and confer to the extent any Party seeks limitations on the scope of its preservation duties.

5. Collection and Review

5.1 The Parties agree that in responding to an initial and any subsequent Fed. R. Civ. P. 34 request, they will meet and confer about methods to search ESI in order to identify ESI that is subject to production and discovery and filter out ESI that is not subject to discovery, including the selection of appropriate custodians, custodial and non-custodial sources, date ranges, file types, or any additional proposed method to cull documents for review (*e.g.*, search terms, technology-assisted review, predictive coding, artificial intelligence).

5.2 Search Terms. If a Producing Party intends to use search terms to limit its collection, review, or production of ESI, that Party or Non-Party shall

disclose to the Requesting Party the collections of ESI for which it proposes to use search terms and the search terms that it proposes to use for each collection of ESI. The Producing Party shall also make disclosures reasonably necessary for the Requesting Party to assess the efficacy of the proposed search terms, including, but not limited to, (1) the number of documents responsive to the search terms collectively; (2) the number of documents that hit on a specific search term and no other search terms (*i.e.*, unique hit count); and (3) the number of documents responsive to each proposed search term. After receipt of the search terms and disclosures set forth above, the Requesting Party shall raise any concerns and propose any additions or modification it may have to the search terms. The Parties and any Non-Parties shall meet and confer in good faith regarding any proposed changes, and provide updated search term disclosures, consistent with the disclosures described above, addressing proposed additional search terms. Any disputes regarding the use of search terms that cannot be so resolved may be consequently raised with the Court.

5.3 Technology Assisted Review ("TAR"). If any Party or Non-Party wishes to use TAR (including predictive coding or artificial intelligence) to determine whether Documents or ESI are responsive or to otherwise limit the Documents or ESI that it produces, it shall notify the Requesting Party and provide it a proposed TAR protocol, before implementing any TAR

protocol. That TAR protocol shall identify the TAR software name and version and the types of metrics available during the training, overview of the review and training workflow, quality control, and validation processes. These metrics shall include a proposed recall level and a proposed confidence level. The protocol should also include a proposal for non-responsive sampling analysis, with all appropriate metrics for such analysis. After receipt of the TAR protocol set forth above, the Requesting Party shall raise any concerns and propose any additions or modification it may have. The relevant Parties and any Non-Parties shall meet and confer in good faith regarding any proposed changes. Any disputes regarding the use of TAR that cannot be so resolved may be consequently raised with the Court.

Notwithstanding the above, Documents or ESI that are found only in hard copy, are data sets, or are uncategorizable (i.e., Documents that do not have sufficient text, or too much text, to be categorized using TAR) will be reviewed manually, or, in the case of junk files, may be reviewed through statistical sampling.

5.4 Each Producing Party shall use its best efforts to filter out common system files and application executable files by using a commercially reasonable hash identification process. Hash values that may be filtered out during this

process are located in the National Software Reference Library ("NSRL") NIST hash set list.

5.5 Embedded Objects. Each Producing Party may, at their reasonable discretion, filter out embedded objects.

5.6 De-Duplication. Removal of duplicate Documents should only be done on exact duplicated Documents (based on MD5 or SHA-1 hash values, at the family level). Attachments should not be eliminated as duplicates for purposes of production, unless the parent e-mail and all attachments are also duplicates. When applying de-duplication, metadata identifying all custodians in possession of each Document that is removed as a duplicate must be provided in the "Alternative Custodian" metadata field, to the extent applicable. Additionally, all BCC recipients whose names would have been included in the BCC metadata field, to the extent such metadata exists, but are excluded because of de-duplication, must be identified in the BCC metadata field specified in Appendix 1. In the event of rolling production of Documents or ESI, the Producing Party will, as needed supplement the load files with updated Alternative Custodian and file path information, as well as update BCC information to the extent such metadata

exists. Duplicate custodian information may be provided by a metadata overlay and will be provided by a Producing Party on an ongoing basis.

5.7 Email Threading. Where multiple email messages are part of a single chain or "thread," a Producing Party is only required to produce the most inclusive message ("Last In Time Email") and need not produce earlier, less inclusive email messages or "thread members" that are fully contained, including attachments and inline objects (including inline images and hyperlinks) and including identical text, identical subject(s), identical senders and recipients (including in "to," "cc," and "bcc" fields), within the Last In Time Email. Only email messages for which all inline objects, text, subject(s), senders, recipients, and attachments are fully contained in and identical to the relevant portion of the Last In Time Email will be considered less inclusive email messages that need not be produced.

5.8 Hardcopy Documents. In scanning hardcopy Documents, distinct Documents should not be merged into a single record, and single Documents should not be split into multiple records (*i.e.*, hardcopy Documents should be logically unitized).

5.9 Password Protected Files. The Producing Party shall make reasonable efforts to ensure that encrypted or password-protected Documents are processed for review and production under the requirements of this ESI Stipulation and Order, and that the decrypted Document is produced if

responsive and not privileged. To the extent such a Document is not successfully processed and is either attached to another Document meeting production criteria or itself has extractable metadata meeting production criteria, the Producing Party agrees to: (i) produce a slipsheet for each encrypted or password-protected Document that cannot be successfully processed indicating that the Document cannot be decrypted; and (ii) provide the metadata for the Document required by Exhibit 1 to the extent it can be reasonably extracted from the file in its encrypted form. The encrypted native version of the Document or ESI need not be produced.

5.10 Filtering. If a Producing Party proposes to apply filters to limit Documents and ESI that is collected for processing and review other than those described in this Order, the Producing Party shall advise all Requesting Parties and the Requesting and Producing Parties shall meet and confer regarding such additional proposed filters.

6. Production Format

Producing Parties produce Documents and ESI in the formats described in Appendix 1 to this Order. If particular Documents or ESI warrant a different format, the Parties and any Non-Parties shall cooperate to arrange for the mutually acceptable production of such Documents or ESI. To the extent practicable, Producing Parties shall not materially degrade the searchability of Documents or ESI as part of the production process.

7. **Privilege Log**

7.1 The Producing Party shall provide the Requesting Party with a log in Excel format of the Documents withheld for privilege containing the following information, to the extent reasonably available: document number, custodian, author/sender, recipient, CC recipient, BCC recipient, date sent, date created, date last modified, file path(s), last edited by, hash value, file name, subject, and time, subject, Privilege Basis and Privilege Justification.

7.2 "Privilege Basis" refers to the legal basis for withholding the document (*e.g.*, Attorney-Client Communication, Attorney Work Product). "Privilege Justification" refers to a description justifying the Privilege Basis, including as appropriate, the subject matter of the legal advice, and/or the litigation matter for which the Document was prepared. To the extent a common interest is asserted, that shall be indicated in the Privilege Basis. The same Privilege Justification may be used for multiple Documents so long as the Privilege Justification is accurate.

7.3 Parties must identify lawyers and third parties on their privilege logs. Parties must identify lawyers in one of two ways: (1) they may provide the other Party with a list with the privilege log that names the lawyers on the log, identifying whether they are in-house or external counsel, or (2) they may designate in-house attorney names with an asterisk and designate outside counsel attorney names with a double asterisk. To the extent

attorneys are not identified in the above fields, they shall be identified in a separate "Attorneys" field.

7.4 Information to be included in the log may be generated from available Metadata so long as: (a) it is reliable and does not contain information that is privileged or protected; and (b) the following additional metadata fields are included (if reasonably available): (i) file path(s); (ii) last edited by; (iii) hash value; (iv) file name; and (v) subject.

7.5 A single Document containing multiple Email messages (*i.e.*, an Email chain) may be logged as a single entry with all sender and recipient information for only the most inclusive Email messagee if the entire chain is privileged. If only part of a chain is privileged, the privileged content should be redacted and the remaining content in the chain should be produced.

7.6 A Document Family (*e.g.*, an Email and its attachments) may be logged as a single entry so long as the entire Family is privileged and the log entry accurately describes both the Parent and its attachment(s) in the manner required by Rule 26(b)(5)(A)(ii).

7.7 Documents that need not be logged are identified in the Protective Order.

7.8 Notwithstanding the foregoing, log entries contained in final privilege logs produced during the Government Plaintiffs' pre-complaint investigations

need not be included in subsequent privilege logs and need not automatically be reformatted consistent with this ESI Stipulation and Order.

IT IS THEREFORE ORDERED that the Joint Motion for Entry of a Stipulated Order Regarding the Discovery of Electronically Stored Information [Doc. #115] is GRANTED and the Stipulated Order is ADOPTED as set out above.

This, the 28th day of May, 2024.

/s/ Joi Elizabeth Peake
United States Magistrate Judge

APPENDIX 1: PRODUCTION FORMAT

1. A cover letter shall be included with each production and shall include information sufficient to identify all accompanying media (hard drive, thumb drive, DVD, CD, secure FTP), shall identify each production on such media by assigning a Production Volume name or number, shall include the Bates range for the Documents produced in each volume, and shall include a list of load file fields in the order in which they are organized in the load file.
2. Except for privileged material, the Producing Party will produce each responsive document in its entirety by including all shared-drive hyperlinks (if reasonably available) and attachments and all pages, regardless of whether they directly relate to the specified subject matter. Attachments must be produced along with the document to which they are attached and/or linked. Hyperlinked documents will be produced along with the document that links to them to the extent the hyperlinked document can be reasonably and automatically exported with the original document at the time of collection. In the event that a hyperlinked document is not produced with the file to which it is linked, the Producing Party will meet and confer about producing it in response to a specific request from the Requesting Party. Copies that differ in any respect from an original (because, by way of example only, handwritten or printed notations have been added) should be produced separately.

3. Form of Production. Documents stored in electronic or hard-copy formats in the ordinary course of business shall be submitted in the following electronic format, in color to the extent kept in color in the ordinary course, provided that such copies are true, correct, and complete copies of the original documents:

    a) Submit spreadsheet (e.g., Excel), presentation (e.g., PowerPoint), and media (e.g., .mp4), and word processing documents with tracked changes (but only if track changes information do not appear in image format productions), files in native format with extracted text and metadata, except if any such files are being redacted, in which case redacted presentation files may be produced as single page 300 DPI TIFF/ JPG images (JPG if in color). Delimited text files and files exceeding 999 pages when imaged may also be produced in native format. For each native file produced, the production will include a *.tiff image slipsheet indicating the production number of the native file and the confidentiality designation, and stating "File Provided Natively." Submit the following metadata and information for native files as applicable (to the extent reasonably available):

Metadata/Document Information	Description
Alternative Custodian	List of custodians where the document has been removed as a duplicate.
Bates Begin	Beginning Bates number of the email.
Bates End	Bates number of the last page of the email.
Beg Attach	First Bates number of attachment range.
End Attach	Ending Bates number of attachment range.
Custodian	Name of the person from whom the email was obtained.

Metadata/Document Information	Description
Email BCC	Names of person(s) blind copied on the email.
Email CC	Names of person(s) copied on the email.
Email Date Received	Date the email was received. [MM/DD/YYYY]
Email Date Sent	Date the email was sent. [MM/DD/YYYY]
Email From	Names of the person who authored the email.
Email Message ID	Microsoft Outlook Message ID or similar value in other message systems.

Metadata/Document Information	Description
Email Subject	Subject line of the Email or Calendar Invite
Email Time Received	Time email was received. [HH:MM:SS AM/PM]
Email To	Recipients(s) of the email.
Email Time Sent	Time email was sent. [HH:MM:SS AM/PM]
Page count	Number of pages in record.
File size	Size of document in KB.
File Extension	File extension type (*e.g.*, docx, xlsx).

Metadata/Document Information	Description
Record Type	Indicates form of record: E-Doc, E-Doc Attachment, Email, Email Attachment, HardCopy, Calendar Appt, Text Message, Chat Message etc.
Folder	File path/folder location of email.
Hash	Identifying value used for deduplication – typically SHA1 or MD5.
Redaction	Indicates Yes or No status regarding document redactions.
Text Link	Relative path to submitted text file. Example: \TEXT\001\FTC0003090.txt
Confidentiality	Confidentiality designation pursuant to the Protective Order.

b) Submit emails in 300 DPI TIFF (Group IV) format with extracted text and the following metadata and information as applicable (to the extent reasonably available):

Metadata/Document Information	**Description**
Alternative Custodian	List of custodians where the document has been removed as a duplicate.
Bates Begin	Beginning Bates number of the email.
Bates End	Bates number of the last page of the email.
Beg Attach	First Bates number of attachment range.
End Attach	Ending Bates number of attachment range.

Metadata/Document Information	Description
Custodian	Name of the person from whom the email was obtained.
Email BCC	Names of person(s) blind copied on the email.
Email CC	Names of person(s) copied on the email.
Email Date Received	Date the email was received. [MM/DD/YYYY]
Email Date Sent	Date the email was sent. [MM/DD/YYYY]
Email From	Names of the person who authored the email.

Metadata/Document Information	Description
Email Message ID	Microsoft Outlook Message ID or similar value in other message systems.
Email Subject	Subject line of the Email or Calendar Invite
Email Time Received	Time email was received. [HH:MM:SS AM/PM]
Email To	Recipients(s) of the email.
Email Time Sent	Time email was sent. [HH:MM:SS AM/PM]
Page count	Number of pages in record.
File size	Size of document in KB.

Metadata/Document Information	Description
File Extension	File extension type (*e.g.*, docx, xlsx).
Record Type	Indicates form of record: E-Doc, E-Doc Attachment, Email, Email Attachment, HardCopy, Calendar Appt, Text Message, Chat Message etc.
Folder	File path/folder location of email.
Hash	Identifying value used for deduplication – typically SHA1 or MD5.
Redaction	Indicates Yes or No status regarding document redactions.
Text Link	Relative path to submitted text file. Example: \TEXT\001\FTC0003090.txt
Confidentiality	Confidentiality designation pursuant to the Protective Order.

c) Submit email attachments other than those described in subpart in subpart 3.a) in 300 DPI TIFF (Group IV) format. For all email attachments, provide extracted text and the following metadata and information as applicable (if reasonably available):

Metadata/Document Information	**Description**
Alternative Custodian	List of custodians where the document has been removed as a duplicate.
Bates Begin	Beginning Bates number of the document.
Bates End	Last Bates number of the document.
Beg Attach	First Bates number of attachment range.
End Attach	Ending Bates number of attachment range.

Metadata/Document Information	Description
Custodian	Name of person from whom the file was obtained.
Date Created	Date the file was created. [MM/DD/YYY]
Date Modified	Date the file was last changed and saved. [MM/DD/YYYY]
Page count	Number of pages in record.
File size	Size of document in KB.
File Extension	File extension type (*e.g.*, docx, xlsx).
Filename with extension	Name of the original native file with file extension.

Metadata/Document Information	Description
Record Type	Indicates form of record: E-Doc, E-Doc Attachment, Email, Email Attachment, HardCopy, Calendar Appt, Text Message, Chat Message etc.
Hash	Identifying value used for deduplication – typically SHA1 or MD5.
Author	Author field value extracted from the metadata of a native file
Last Author	Last Saved By field value extracted from metadata of a native file
Redaction	Indicates Yes or No status regarding document redactions.
Native Link	Relative file path to submitted native or near native files. Example: \NATIVES\001\FTC0003090.xls

Metadata/Document Information	Description
Parent ID	Document ID or beginning Bates number of the parent email.
Text Link	Relative path to submitted text file. Example: \TEXT\001\FTC0003090.txt
Time Created	Time file was created. [HH:MM:SS AM/PM]
Time Modified	Time file was saved. [HH:MM:SS AM/PM]
Confidentiality	Confidentiality designation pursuant to Protective Order.

d) To the extent instant messages (*e.g.*, text messages, WhatsApp, Slack, iMessage, Teams, G-Chat, Bloomberg, etc.) are produced, a Party shall produce such messages such that individual messages are grouped into threads (*i.e.*, continuous conversations between one or more individuals) of

24 hours to allow for the full context of conversations to be visible. Submit instant messages in native or TIFF Relativity Short Message Format ("RSMF") accompanied by extracted text if available, or OCR, and the following metadata (if reasonably available) and meet and confer regarding any additional metadata fields that could be produced, depending on the type of message:

Metadata/Document Information	**Description**
Instant Message Type	The type of electronic message (*e.g.*, Text Message, Slack, Microsoft Teams, Instant Bloomberg, etc.)
Instant Message Participants	Senders, recipients, subscribers, or others who have the ability to participate in a group message or channel
Instant Message Subject	Subject or name of the messaging thread or topic, if any
Instant Message Channel	Name of persistent messaging group or chat room, if any
Instant Message Date	Date of last instant message in the 24-hour thread
Confidentiality	Confidentiality designation pursuant to the Protective Order.

e) Submit all other electronic documents, other than those described in subpart 3.a), in 300 DPI TIFF (Group IV) format accompanied by extracted text and the following metadata and information as applicable (if reasonably available):

Metadata/Document Information	Description
Alternative Custodian	List of custodians where the document has been removed as a duplicate.
Bates Begin	Beginning Bates number of the document.
Bates End	Last Bates number of the document.
Beg Attach	First Bates number of attachment range.
End Attach	Ending Bates number of attachment range.
Custodian	Name of the original custodian of the file.

Metadata/Document Information	Description
Date Created	Date the file was created. [MM/DD/YYY]
Date Modified	Date the file was last changed and saved. [MM/DD/YYYY HH:MM:SS AM/PM]
Record Type	Indicates form of record: E-Doc, E-Doc Attachment, Email, Email Attachment, HardCopy, Calendar Appt, Text Message, Chat Message etc.
Author	Author field value extracted from the metadata of a native file
Last Author	Last Saved By field value extracted from metadata of a native file
Redaction	Indicates Yes or No status regarding document redactions.
Page count	Number of pages in record.

Metadata/Document Information	Description
File size	Size of document in KB.
File Extension	File extension type (*e.g.*, docx, xlsx).
Filename with extension	Name of the original native file with file extension.
Hash	Identifying value used for deduplication – typically SHA1 or MD5.
Originating Path	File path of the file as it resided in its original environment.
Production Link	Relative path to submitted native or near native files. Example: \NATIVES\001\FTC0003090.xls

Metadata/Document Information	Description
Text Link	Relative path to submitted text file. Example: \TEXT\001\FTC-0003090.txt
Time Created	Time file was created. [HH:MM:SS AM/PM]
Time Modified	Time file was saved. [HH:MM:SS AM/PM]
Confidentiality	Confidentiality designation pursuant to the Protective Order.

f) Submit documents stored in hard copy in 300 DPI TIFF (Group IV) format accompanied by OCR with the following information:

Metadata/Document Information	Description
Bates Begin	Beginning Bates number of the document.
Bates End	Bates number of the last page of the document.
Record Type	Indicates form of record: E-Doc, E-Doc Attachment, Email, Email Attachment, HardCopy, Calendar Appt, Text Message, Chat Message etc.
Page count	Number of pages in record.
Redaction	Indicates Yes or No status regarding document redactions.
Custodian	Name of person from whom the file was obtained.
Confidentiality	Confidentiality designation pursuant to the Protective Order.

g) Submit redacted documents in TIFF/JPG format accompanied by extracted text or OCR with the metadata and information required by relevant document type in subparts 3.a-f) above.

h) Documents produced as TIFFs/JPGs will show any and all non-privileged text, hidden content, and images that would be visible to the reader using the native software that created the document, including any tracked changes, comments, speaker notes, and hidden content.

4. For requests in which responsive information is contained in a database (*e.g.*, Microsoft Access) or other structured or aggregated data source or otherwise maintained by an application, the Parties shall meet and confer as to whether a Party may produce relevant information by generating one or more reports used in the ordinary course of business. If the Requesting Party believes that the generation of ordinary course reports is not adequate, the relevant Parties agree to meet and confer to discuss alternative forms of production. If the relevant Parties cannot reach agreement, the matter may be submitted to the Court for resolution.

5. Compressed file types (e.g., .ZIP, .RAR, .CAB, .Z) should be decompressed so that the lowest level document or file is extracted.

6. Produce ESI submissions as follows:

a) For productions over 500 gigabytes, use an External Hard Disc Drive (stand-alone portable or hard drive enclosure) or USB Flash Drive in Microsoft Windows-compatible, uncompressed data format.

b) For productions under 500 gigabytes, submissions may be transmitted electronically via secure File Transfer Protocol, such as Kiteworks or Globalscape.